

Private Malware for Sale: A Closer Look at AresLoader

By Flashpoint Intel Team

Published: 2023-03-06 · Archived: 2026-04-05 15:04:42 UTC

A new private loader for sale

In December 2022, a private loader named “AresLoader” was advertised for sale on the top-tier Russian-language hacking forum XSS by a threat actor going by the name “DarkBLUP”. The seller claimed that they were selling access to the malware for \$300 per month and were only issuing ten licenses at a time.

According to DarkBLUP, AresLoader is designed to camouflage itself as legitimate software while covertly downloading harmful payloads. The sales ad also revealed that AresLoader operates through a single command and control (C2) panel that receives logs, and customers can create user accounts for the panel.



Sales thread posted to XSS by DarkBLUP. (Source: Flashpoint)

The AresLoader sellers have also set up a Telegram channel to facilitate discussions related to the bot. The IP address of the C2 server indicates that it belongs to an autonomous system number (ASN) registered to the bulletproof hosting provider Partner LLC.

How AresLoader works

Flashpoint analysts have evaluated a sample build of AresLoader and confirmed that it performs the advertised functions.

```
.text:0040167B      mov     eax, ds:__imp__Sleep@4 ; Sleep(x)
.text:00401680      call   eax ; Sleep(x) ; Sleep(x)
.text:00401682      sub     esp, 4
.text:00401685      mov     eax, [ebp+1Path]
.text:00401688      mov     [esp+4], eax ; dwnPath
.text:0040168C      mov     dword ptr [esp], offset __Z18legitur1 ; url
.text:00401693      call   __Z13DownloadFilesPKc58_ ; DownloadFiles(char const*,char const*)
.text:00401698      mov     eax, [ebp+1Path]
.text:0040169B      mov     [esp], eax ; file
.text:0040169E      call   __Z28ExecuteLegitProgramPKc ; ExecuteLegitProgram(char const*)
.text:004016A3      mov     eax, [ebp+pPath]
.text:004016A6      mov     [esp+4], eax ; dwnPath
.text:004016AA      mov     dword ptr [esp], offset __Z110payloadur1 ; url
.text:004016B1      call   __Z13DownloadFilesPKc58_ ; DownloadFiles(char const*,char const*)
.text:004016B6      mov     eax, [ebp+pPath]
.text:004016B9      mov     [esp], eax ; file
.text:004016BC      call   __Z25ExecutePayloadEXEProgramPKc ; ExecutePayloadEXEProgram(char const*)
.text:004016C1      mov     dword ptr [esp+4], offset fileNameReestr
.text:004016C9      mov     eax, [ebp+pPath]
.text:004016CC      mov     [esp], eax ; szPath
.text:004016CF      call   __Z9AddRegKeyPKc5_ ; AddRegKey(char *,char *)
.text:004016D4      mov     eax, [ebp+sPath]
```

AresLoader downloader function calls. (Source: Flashpoint)

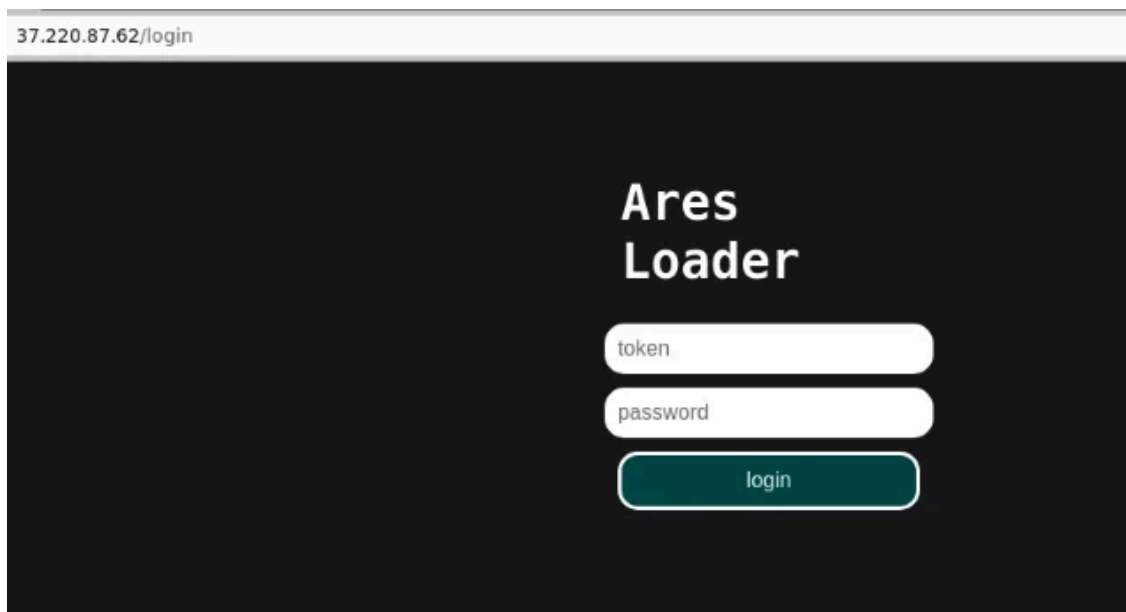
Once dropped on the system, it scrapes the victim device’s IP address and time zone, generates a UUID for the infected system, and beacons out to the C2 server with a POST request. This beacon includes the scraped data mentioned above as well as campaign identifiers such as an ‘owner_token.’

After registering the loader on the C2 server, the loader downloads the expected legitimate file specified during the build’s creation. It executes that file and downloads the additional harmful payloads. The downloaded files are saved in a folder and then executed. AresLoader then creates a Registry AutoRun key to obtain and retain unauthorized access to the victim’s environment.

It is worth noting that the “owner_token” field identifies the AresLoader customer to whom the build belongs. Some customer tokens might be linked to threat actor accounts that were active in various illicit communities collected by Flashpoint over the past two months.

AresLoader panel and server

The AresLoader panel is managed and hosted by the malware seller, and it appears that all AresLoader builds communicate with a single server.



AresLoader login landing page. (Source: Flashpoint)

This server’s IP address has been detected as the recipient of communication consistent with AresLoader’s command and control (C2) functions. Additionally, a file that resembles an AresLoader build has also been observed communicating with this IP address.

What security teams can learn from ASNs

The IP address used by AresLoader’s server belongs to the autonomous system number (ASN) AS204603 and is registered as Partner LLC. Note that the use of “LLC” in the ASN name does not necessarily indicate the company is a registered LLC; it may be part of the name. This ASN exhibits several traits characteristic of bulletproof hosting providers.

Bulletproof hosting providers are similar to standard hosting providers but cater to threat actors who seek to host malicious infrastructure without fear of the servers being taken down due to abuse policies.

Identifying bulletproof hosting provider ASNs can be useful to security researchers and organizations with the ability to block IP ranges. These ASNs’ announced IP ranges are highly unlikely to host legitimate services, making them valuable in identifying malicious infrastructure or preventing malicious activity proactively.

Partner LLC also hosts the “Shark” stealer panel, indicating that the ASN supports other malicious infrastructure besides AresLoader. Additionally, another Partner LLC IP hosts securespend[.]org, a [phishing](#) site masquerading as securespend[.]com.



Shodan result for Shark Stealer Panel. (Source: Shodan)

Protect your organization’s critical infrastructure with Flashpoint

Flashpoint’s suite of actionable intelligence solutions enables organizations to proactively identify and mitigate cyber and physical risk that could imperil people, places, and assets. To unlock the power of great [threat intelligence](#), get started with a [free Flashpoint trial](#).

Source: <https://flashpoint.io/blog/private-malware-for-sale-aresloader/>